A Reproduced Copy

OF

Reproduced for NASA

by the

NASA Scientific and Technical Information Facility

N71 19788

RECONFIGURABLE G & C COMPUTER STUDY FOR SPACE STATION USE

FINAL REPORT

VOLUME I

TECHNICAL SUMMARY

31 January 1971

J. Jurison
Program Manager

Prepared Under Contract No. NAS9-10416

Autonetics Division of North American Rockwell
for
Manned Spacecraft Center
National Aeronautics and Space Administration

FOREWORD

This final report covers the work performed by Autonetics Division of North American Rockwell Corporation under a study contract entitled Reconfigurable G&C computer Study for Space Station Use. The report is submitted to the National Aeronautics and Space Administration Manned Spacecraft Center under the requirements of Contract NAS 9-10416. The study program covered the period from December 29, 1969 through January 31, 1971. The NASA Technical Monitor was Mr. E. S. Chevers.

The final report consists of seven (7) volumes:

Volume I	Technical Summary
Volume II	Final Technical Report
Volume III	Appendix I. Model Specification
Volume IV	Appendix 2. IOP - VCS Detailed Design
Volume V	Appendix 3. System Analysis and Trade-Offs
Volume VI	Appendix 4. Software and Simulation Description and Results
Volume VII	Appendix 5. D-200 Computer Family
	Appendix 6. System Error Analysis
	Appendix 7. Reliability Derivation for Candidate Computers
	Appendix 8. Power Converter Design Data
	Appendix 9. Data Transmission Medium Design

YOU ARE READING THIS VOLUME

VOLUME I
TABLE OF CONTENTS

VOLUME I
LIST OF ILLUSTRATIONS

1.0 INTRODUCTION

1.1 SUMMARY

The purpose of the study is to define the general system requirements and specify the configuration for a modularized reconfigurable, fault tolerant guidance and control computer system suitable for a manned space station complex. The study includes power distribution, modular computing elements at various subsystems, input/output data bus, and the development of necessary software to demonstrate the self-test and reconfiguration ability of the system by computer simulation. This volume contains a summary of the results of the study.

1.2 GENERAL REQUIREMENTS

The computer system is required to support the Guidance and Control (G&C) requirements of the Space Station during each mission phase. The Space Station is expected to operate in a circular 200 - 300 mile orbit of 55 degree inclination with added capability for polar orbits. The mission can be broken down into four major phases: Prelaunch, Boost, Orbit Injection and Orbital Coast.

The orbital coast phase was the phase of primary concern for this study and is used to estimate the memory size, speed, and signal interface requirements for the computer system. The G&C system consists of several subsystems as shown in the functional block diagram, Figure 1-1.

The G&C computer and computing elements at subsystem level perform all computational tasks associated with navigation and attitude control function. Data processing functions associated with the experiments and display and control functions are handled by another computer complex, called the Information Management Data Processor. The latter provides mode control signals and receives navigation data from the G&C computer.

A common multiplexed data bus provides a means of transferring data between the subsystems and the guidance and control computer complex.

The manned environment and long periods of independent operation dictate more stringent reliability requirements than have been imposed upon spacecraft computers in the past. It has to be modular for ease of maintenance and be tolerant to three failures in a fail op, fail op, fail safe manner. This means that it must be able to detect failures, isolate failures to a modular level, and recover from failures by reconfiguring the system (replacing the faulty module with a spare).

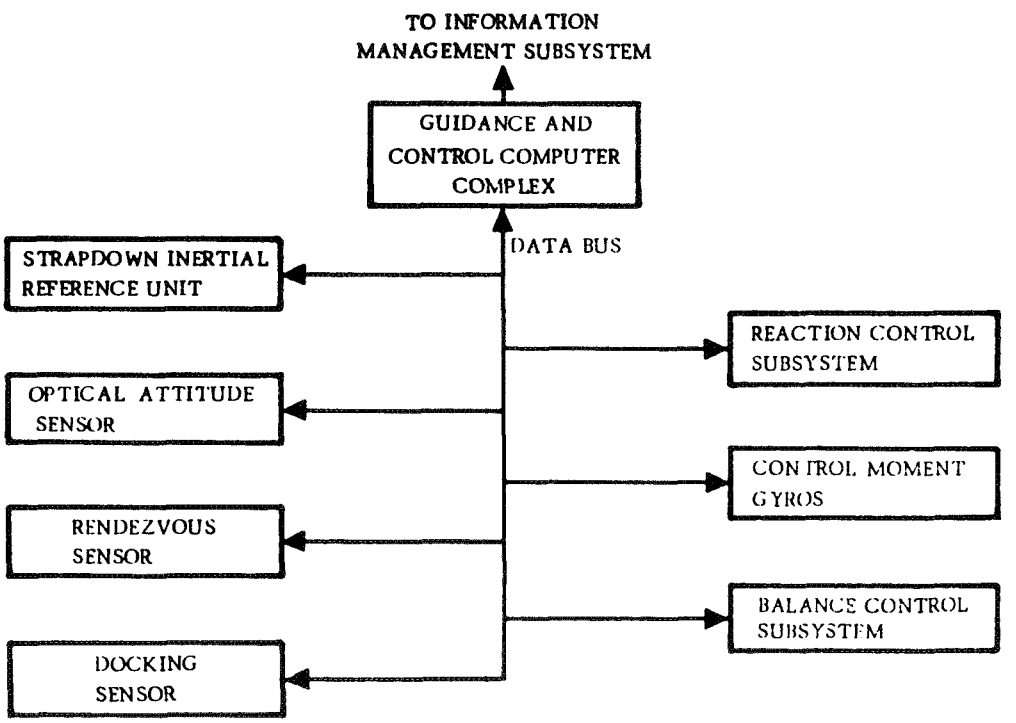

FIGURE 1-1. FUNCTIONAL BLOCK DIAGRAM , G&C SYSTEM

2.0 TECHNOLOGY REVIEW

2.1 OBJECTIVE

In order to establish a technological baseline for system tradeoffs in the study, a brief technology review was conducted. The review covered three areas: semiconductor logic technologies, memory technologies (magnetic and semiconductor), and packaging. General ground rules for the review were that technologies considered should be producible in 1972 and that no substantial development should be required. Reliability was considered the most important factor in evaluating a technology but other characteristics important to spaceborne systems such as size, weight, and power were also covered.

2.2 SEMICONDUCTOR LOGIC TECHNOLOGY

Semiconductor technologies under consideration for use in logic portions of the Reconfigurable Computer have been limited to those with proven reliability and producibility. Three technologies, bipolar, P-channel MOS, and complementary MOS (CMOS) fall into this category. Both bipolar and P-channel circuits are currently being produced by a large number of manufacturers and therefore represent virtually zero risk. CMOS, because of the limited number of suppliers, must be considered as a slightly higher risk.

The reliability of a system can be greatly enhanced by reducing the number of connections required. One method of accomplishing this is to increase the level of integration on the semiconductor devices to reduce interface signals. Of the three technologies being considered, P-channel MOS is capable of the highest of integration, approximately twice that achievable with either bipolar or CMOS technoligies.

Power is also an important reliability factor in integrated circuits. Many failure modes are accelerated by high temperatures. It is desirable to keep chip temperatures low by using low power circuit techniques. Both 4-phase P-channel MOS and CMOS have very low power dissipations. Bipolars generally have high power dissipations, e.g., a large array may dissipate 1 watt of power limiting the number of bipolar arrays that can be mounted on a substrate.

It is concluded that P-channel MOS is the most suitable semiconductor logic technology for the Reconfigurable G&C Computer. The technology is well established and is capable of the highest levels of integration. It is compatible with high reliability interconnect techniques and is low power when a 4-phase clocking circuit mechanization is used. This permits high density packing which minimizes both size and weight of the system.

2.3 SEMICONDUCTOR MEMORIES

Recent developments, particularly in the MOS area, have increased density and reduced power and cost of semiconductor memories to a point where they can effectively compete with magnetics in small capacity memories such as the Local Processor memory. Both read/write (RWM) and read-only (ROM) memories were investigated.

The highest density random access read/write semiconductor memories currently available are P-channel MOS devices. Devices for 64 to 1024 bits are currently available or will be in the very near future. Access times range from 60 usec to about 1 usec and the power dissipation is .5 to 2 mw/bit during access. In read/write semiconductor memories where the standby power is of prime importance, CMOS becomes a strong candidate. At the present time, CMOS offers the lowest standby power of all semiconductor memories. CMOS memory devices still suffer from lower packing density than is possible from single channel MOS. The largest CMOS memory device reported is a 256-bit array on a 17,400 sq. mil die. Access time is approximately 305 nsec. The above 256-bit array is not generally available today but it is reasonable to expect CMOS memories of this density to be producible in 1972.

In applications requiring high speed memory access, bipolar semiconductor memory circuits may be required. Several manufacturers are currently producing 64-bit bipolar memory devices. The typical acces times for these chips is 60 nsec. The penalty for this speed is power. Typical power dissipations are 5 to 6 mw/bit.

Very compact ROM's can be produced using the MOS technology. 4096 bit ROM's are currently available. MOS ROM arrays are very similar to diode arrays. The presence or absence of an MOS device or a diode denote whether a one or a zero is stored. A single bit of storage can occupy as little as 1.5 $mils^2$. The read access time for typical 4096 bit ROM is less than 500 nsec with a total memory cycle time of about 800 nsec. MOS ROM speeds are a strong function of the array size, larger arrays being correspondingly slower.

Considerable industry wide interest exists in an electrically alterable read only memory produced using the MNOS process. MNOS memories are non-volatile and have very low standby power. Read access times are expected to be about 0.5 microseconds in large arrays but write times have thus far been very slow (1 msec). The technology is therefore being considered only for ROM applications in normal computer systems. The MNOS storage mechanism involves the switching of the threshold voltage of an MNOS field effect transistor. The hysteresis in this switching action make the devices suitable for memory applications. It is reasonable to expect 100 x 100 mil arrays to contain 1024 bits of MNOS memory. This technology is still developmental at the present time. It cannot be considered as producible in 1972 without significant risk.

2.4 MAGNETIC MEMORIES

Magnetic memories considered for this application may be broken down into three categories:

1. Core
2. Plated Wire
3. Thin Film

Memory module investigated ranged from 2K to 16K words of 24 to 36 bits each. Cycle time of 1 usec with 0.5 usec access time was considered adequate for this application. A 2-1/2 D memory organization was chosen for each case. This choice is best for the plated wire and thin film technologies but it is a debatable choice for core systems of less than the 16K word capacities.

Each of the three technologies was evaluated on several criteria that is of importance in achieving the goals of the Reconfigurable G&C Computer.

Both plated wire and core memories are in production at present and presents no or low technical risk. Plated wire is equal to core memories from volume, weight and cost standpoint. However, it offers substantial advantages over core memories from power, transient immunity and reliability aspects.

Thin film technology is still "just around the corner" for most companies. Yield problems and low output signals still are not completely solved. For a system requiring very low power and very small size, this technology might be a good choice. However, there would be a development effort and a high technical risk.

Based upon the evaluation both plated wire and core memories could meet system requirements at low or no development risk. Although similar in some areas, plated wire memories have definite advantages in areas such as power, reliability and transient failure tolerance. Therefore, it is recommended as the prime candidate for magnetic memory systems in the Reconfigurable G&C Computer system.

2.5 PACKAGING

The packaging technologies review covered interconnections and individual semiconductor circuits as well as module interconnections. Beam lead devices mounted on ceramic substrates are recommended for the Reconfigurable G&C Computer system. Several methods of interconnecting ceramic substrates were investigated. The final choice of the packaging method depends greatly on the overall system requirements and should be left for the computer design engineer.

3.0 SYSTEM ANALYSIS AND TRADE-OFFS

3.1 OBJECTIVES AND BASELINE SYSTEM DESCRIPTION

The purpose of this portion of the study was to investigate the total computational requirements of the G&C system and determine the degree of decentralization for the computer system. The computational requirements of the system shown in Figure 1-1 can be satisfied with several different computer organizations ranging between these two extremes:

(1) A highly centralized system with a powerful computer complex which communicates directly with sensor elements and actuators.

(2) A highly decentralized system in which each sensor and actuator subsystem has its own local processor performing the control computations and checkout functions associated with that subsystem.

Between these extremes, there is room for several variations. For example, the local processor could be nothing more than a data compression and multiplexer device necessary for interfacing with the data bus. On the other hand, it could be a general purpose computer consisting of a processor, memory and "standard interface unit".

The effort consisted of a computational requirements analysis followed by a trade-off phase in order to determine the optimum allocation of computational functions. In addition, an error analysis was performed to determine the effect of correlated horizon sensor measurements or orbit determination

Four subsystems were selected for detailed analysis: (a) Strapdown Inertial Reference Unit (SIRU); (b) Optical Attitude Subsystem (OAS); (c) Control Moment Gyros (CMG's) and (d) Reaction Control Subsystem (RCS).

1. Strapdown Inertial Reference Unit (SIRU)

The inertial reference system uses six single degree of freedom gyroscopes and six linear accelerometers in a dodecahedron array. The principal merits of this configuration is that it offers failure isolation of up to two out of six of both types of instruments and continuous system operation with up to three out of six failures. Furthermore, when all instruments are operating, the redundancy permits cancellation of some error sources associated with the strapdown operation.

2. Optical Attitude Sensors (OAS)

The OAS subsystem includes both star trackers and horizon scanners. The star tracker measurements are used to provide attitude corrections while horizon scanner measurements are combined with computed state

3.1 (continued) - vector to update the estimate of the space vehicle state. Two two-degree of freedom gimbal systems are used to hold two star tracker heads and two horizon scanner heads with each head mounted rigidly with respect to others.

3. Control Moment Gyros (CMG's)

The CMG subsystem was assumed to have three two-degree of freedom control moment gyros configured for zero net angular momentum at gimbal nulls for purposes of accommodating local vertical and artificial "g" mission modes. The subsystem is used for attitude hold and low rate maneuvering. When the gyro gimbal output axes have precessed away from the nominal valve, momentum dumping or desaturation is implemented with RCS subsystem to restore the gimbal output axes to the vicinity of their original position.

4. Reaction Control Subsystem (RCS)

The Reaction Control Subsystem contains sixteen (16) reaction jets arranged in four orthogonal quad stations. The jets are arranged to produce pure couples about the three control axes under normal operation. The RCS is used to remove high rate transients, provide higher attitude maneuver rates, desaturate the CMG's and provide translation for orbital makeup/stationkeeping.

3.2 COMPUTER REQUIREMENTS

To determine the computer requirements, detailed flow diagrams were developed to determine the relationship between each computational task. For functions involving the SIRU, OAS, RCS and CMGs, mechanization equations were developed and estimates were made of the number and types of instructions necessary to solve each equation. For remaining functions, data from previous computer programs was extrapolated or new equations were derived in cases where no previous data existed. The results were compiled in terms of computer memory requirements (instructions, constants, and data) and the number of times each instruction was executed per second. The latter figure was normalized to equivalent short instruction rates, which corresponds to a number of short instructions, such as Add, per second.

The results of the computer requirements analysis are presented in Figure 3.1. The bar on the left represents computer requirements for a system without local processing capability at the subsystem level while the right column represents the other extreme, where the central processor functions have been minimized by performing as many functions at the subsystem level as possible. For the second case, only four subsystems were selected as candidates for performing computations at subsystem level and were subject to detailed analysis and trade-offs: SIRU, OAS, RCS and CMGs.

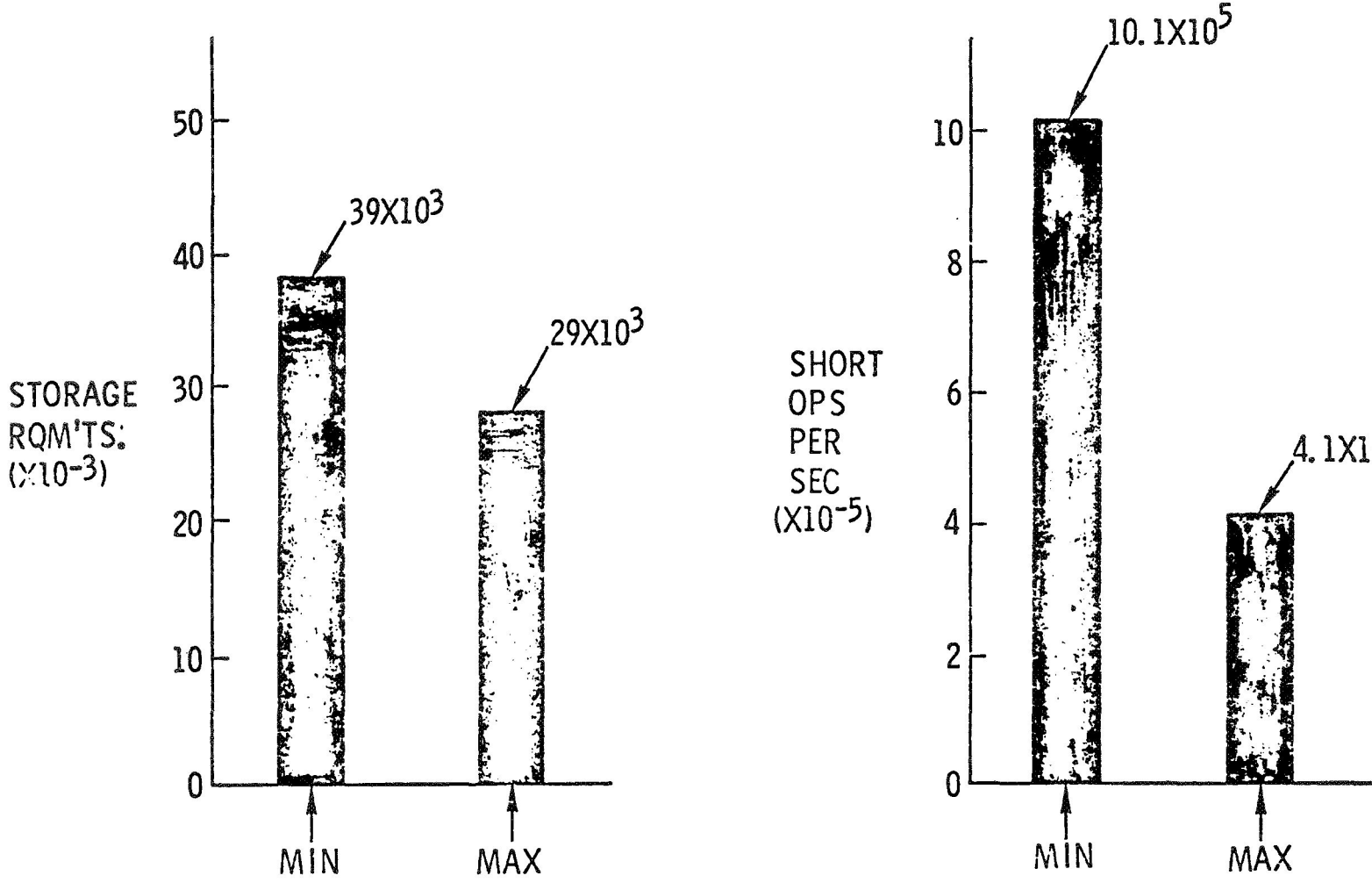

FIGURE 3-1. COMPUTER REQUIREMENTS FOR SYSTEMS WITH MINIMUM AND MAXIMUM PREPROCESSING

3.2 (continued)

It is seen from Figure 3-1 that by preprocessing at subsystem level for the four specific subsystems investigated, the central computer requirements can be reduced by 10,300 words of memory and 604,000 equivalent short operations. The significant reduction in requirements is the effective reduction of speed to the level where it is within the state-of-the art of aerospace computer technology. The reduction in memory capacity at the central computer will become more significant when one considers the fact that the central computer complex will be mechanized with redundant computers, while at the subsystem level the degree of computer redundancy might be lower than at the central processor.

3.3 COMPUTATIONAL TRADE-OFFS

The optimum allocations of computations lies somewhere between the two cases of maximum and minimum preprocessing. The trade-off phase was concerned with the problem of determining the best split of these tasks between the central processor and the local processor dedicated to each of the four subsystems.

The following objectives and criteria were established for performing these trade-offs.

1. Minimization of hardware complexity.
2. Minimization of I/O data rates.
3. Minimization of management interface affecting:
   (a) Number of interface signals
   (b) Technical data exchange
4. Reduction of central computer load
5. Maximization of reliability
6. Maximization of programming efficiency including impact of program changes.

The computational blocks which could be located either in the local processor or the central computer were listed and were grouped in such a way that they were consistent with the basic objectives of the study. The requirements for the local processor were then determined in terms of memory, speed, I/O bus data rate, and number of interface signals. The computational allocation was then selected that satisfied best the evaluation criteria. Figure 3-2 shows the recommended split of computations between the central G&C processor and local processor.

It was concluded from this analysis that the central G&C computer requirements can be reduced to a level where they are within the state-of-the-art of present aerospace computer technology by employing local processors in subsystems. By allocating the computations, as described

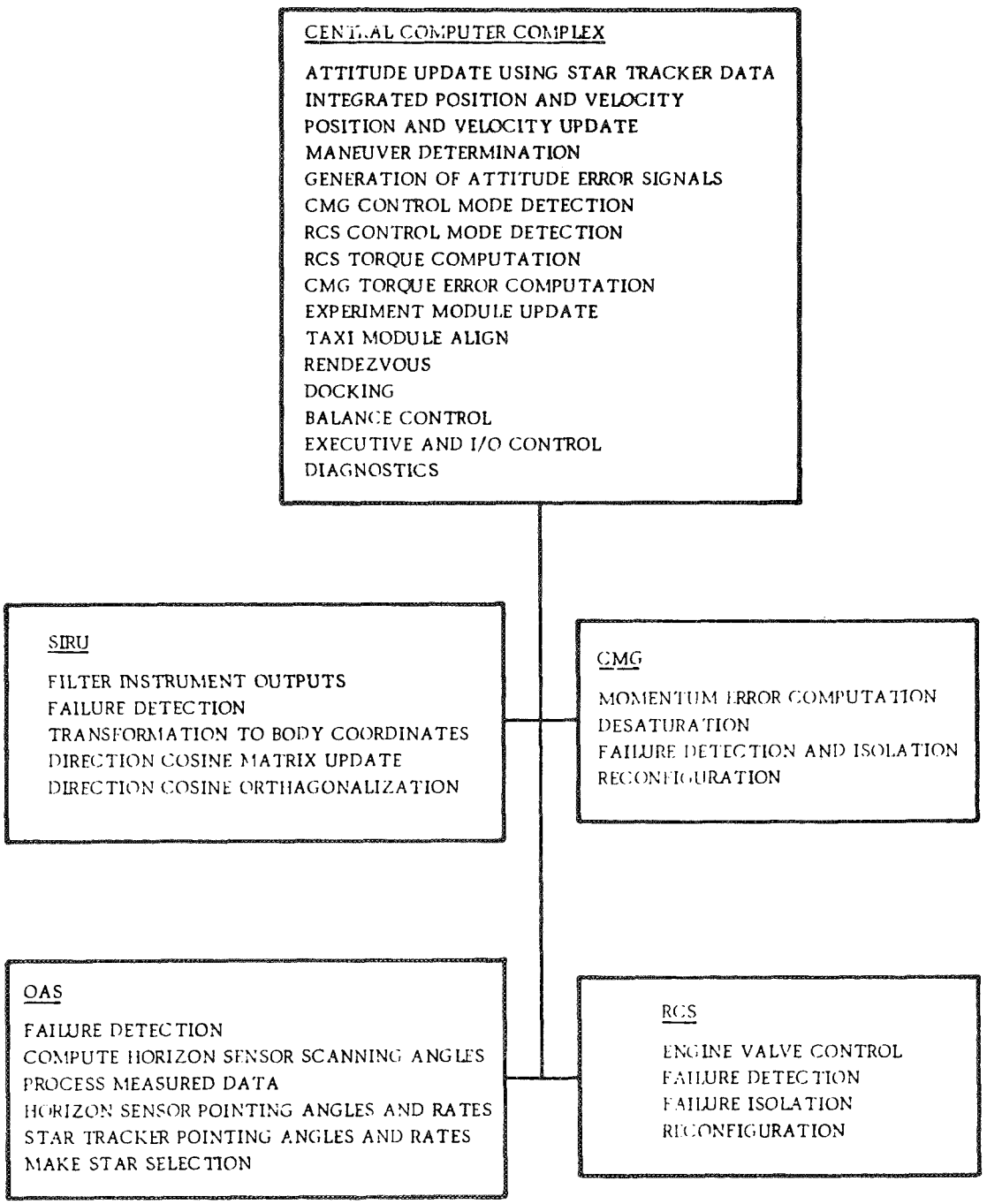

FIGURE 3-2. RECOMMENDED ALLOCATION OF COMPUTATIONAL TASKS

3.3 (continued) - above, the central computer complex will require as a minimum 29,600 words of memory and be capable of executing 500,000 operations per second with the recommended computational allocation. The data rate requirement for the I/O data bus is reduced to approximately 88,000 bits per second. This figure represents only the actual data transmitted and does not include any overhead such as control, address and error detection and/or correction bits. A standardized local processor design with functional characteristics shown in Table 1-1 can satisfy the preprocessing requirements of the subsystems investigated without resulting in a proliferation of on-board computer systems and excessive development costs. The local processor can be mechanized with state-of-the-art LSI technology and would introduce no significant size, weight and power penalties in the overall G&C system.

The approach offers several advantages over conventional centralized computer organizations presently employed in aircraft avionics systems:

1. Reduction of Development Risk. The requirements can be met by state-of-the-art computer technology of moderate speed and memory capacity.

2. Management Interface Clarity. The subsystem interfaces are reduced to a level where they can be explicitly defined early in the program. Subsystem checkout and sell-off is greatly simplified by this approach.

3. Reduced Data Bus Rates. The traffic on the data bus is greatly reduced. A bus system designed for 1 MHz data rate can adequately handle any overhead and expected growth requirements.

4. Reduced Development Cost. Standard local processor design will reduce or eliminate requirements for any special purpose logic required at the subsystem level.

5. Flexibility. Most subsystem hardware changes can be absorbed by the local processor programs and will not reflect back into the central computer programs.

6. Growth Potential. The system can be expanded easily by adding more local processors.

7. Programming Ease. The subsystem supplier can program his own local processor, since he is most familiar with the computer requirements at that level and will be able to handle subsystem changes at minimum cost.

3.3 (continued) -

TABLE 3-1. RECOMMENDED LOCAL PROCESSOR FUNCTIONAL CHARACTERISTICS.

TYPE	GENERAL PURPOSE
Word Length	16-bits
Memory (Read Only) Memory (Read/Write)	4096 words 512 to 1024 words
Speed - Add Time Speed - Multiply Time	2.5 usec. 10.0 usec.
Instruction Set	Conventional plus double precision add, subtract, store, fetch
Number of SIU's	4
Input - Digital	16-bit parallel channel 8 discretes
Input - Analog Output - Digital	8 channel 16-bit parallel channel 8 discretes

3.4 ERROR ANALYSIS

The system analysis effort included a brief study of orbit determination using correlated horizon sensor measurements. The measurements consist of the angle between the line of sight from the spacecraft to the earth's horizon and a fixed line in inertial space such as the line to an appropriately chosen star. The plane defined by these two lines must be perpendicular to the earth's horizon at the point of intersection of this plane and the horizon. The difference between the observed value of this angle and the value computed based on the estimated spacecraft position provides information for updating the state (position and velocity) of the spacecraft.

3.4 (continued) - errors (cross track and down range) tend to decrease with increasing correlation distance constants. The opposite is true with vertical errors up to the point where the "bias" error caused by the correlation can be estimated and corrected. For correlation distance constants of less than 3000 nm, (actual horizon correlation distance constants are estimated to be on the order of 2500 nm) the error results, for the most part, are within 20% of those for a white noise measurement error (zero correlation distance).

Large initial position and velocity errors (up to 50 nm, 1000 fps initial uncertainties) have little if any effect on final navigation errors after a sufficient number (on the order of 20) measurements have been made. The number of and time between measurements was shown to have a significant effect on the final accuracy and is related to the correlation distance.

4.0 COMPUTER SYSTEM CONCEPT TO MEET FAILURE TOLERANCE REQUIREMENTS

This section presents the basic approach to meeting the stringent failure tolerance requirements. Since the approach taken was at a computer system level, detailed considerations of the internal computer architecture are not presented. Various internal architectures were evaluated and a selected one subject to a detailed design; this activity is presented in Section 5.0.

4.1 FAILURE TOLERANCE REQUIREMENTS

In the design of a reliable, failure-tolerant computer system, there are two very basic factors to consider: the amount of failures that are to be tolerated and the reliability of the system. Either one or both of these attributes may be specified as the design goals. The design of the guidance and control computer system for the Space Station program requires triple failure tolerance in a fail-operational, fail-operational, fail-safe (FOOS) manner. Fail operationsl requires that the failure be tolerated with no degradation in performance. Consequently, the failure detection scheme used must provide 1.0 probability of detection and the failure reconfiguration scheme used must be 100 percent effective. Fail safe allows a degradation in performance if crew safety is not impaired. Failure detection requirements remain as stringent; however, failure reconfiguration requirements are eased since only a portion of the failures need be reconfigured rapidly, the remainder allow for a slower reconfiguration process.

The FOOS requirement applies to single failures making the definition of a single failure very important. Since any single failure must be tolerated, all possible failure modes of a module were defined as a single failure. In order to achieve a reasonable design with this requirement, the module must be at a relatively large scale such as a CPU, IOP, Memory, or an entire computer. Additionally, in the design of these modules, extreme caution must be taken to insure that failures are independent.

A minimum level of redundancy of four is required to satisfy the FOOS requirement. The method selected to accomplish failure detection and reconfiguration relies on adaptive voting techniques. The FOOS boundary, for purposes of this study, extended up to the interface with the external subsystems. Consequently, a minimum of four I/O busses must be included in the computer system. Various methods may be used to implement an adaptive voting technique in the computer system. A straight-forward and simple solution is to provide four single computers with four busses to the subsystems and require the subsystems to peform

4.1 (continued) - an adaptive majority vote. Another solution is to provide adaptive majority voters on each of the I/O busses to the subsystems, this approach eases the decision process at the subsystems and is the selected method for the computer system. The differences between the various methods considered in the study involved the method of interconnection between the redundant computers, the technique of performing the adaptive voting, and the location where the adaptive voting was performed.

4.2 SYSTEM CONCEPT

The computer system consists of four computers and four I/O busses that interface with local processors of external subsystems. These computers are interconnected for special I/O functions to achieve a FOOS computer system as shown in Figure 4-1. Each computer contains a connection to one of the four external I/O busses in the system. In addition, each computer contains four interconnections: Three receive channels, one from each of the other computers, and one output channel to all the other computers; it is via these connections that the voter-comparator-switch (VCS) concept is mechanized to implement adaptive voting.

The VCS function is deeply interrelated to the IOP in the computer; however, it may be considered as a unique module. The VCS concept enables the computer system to be operated in a variety of modes: four-way voting (all four computers doing the same job, with one or more of the VCSs voting on the I/O information), three-way voting with the other computer dormant or doing a different job, two-way comparison with the other two computers also in comparison or doing distinct jobs, and four non-redundant computers. The mode is under the control of the executive system which is distributed among all the computers. The executive is redundant, in a distributed sense, to satisfy the FOOS requirement. The level of redundancy of the computations may be changed under software control by changing the mode of the system.

The four computers each operate on its own independent clock. Redundant data operated on by the VCS is required to be in synchronization within a specified tolerance; this data is not required to be in bit sync. The computer system, by a combination of hardware and software, is self-reconfigurable and is capable of withstanding any three failures in a FOOS manner.

4.3 VCS ARCHITECTURE

The VCS device is capable of operating on redundant data in a majority voting or a comparison mode, thereby performing a redundancy reduction of either 4:1, 3:1, or 2:1, or it may operate on non-redundant data. The device is adaptive in that it may be switched into different modes. The device is also adaptive to failures in the computer system by means of adaptive majority logic.

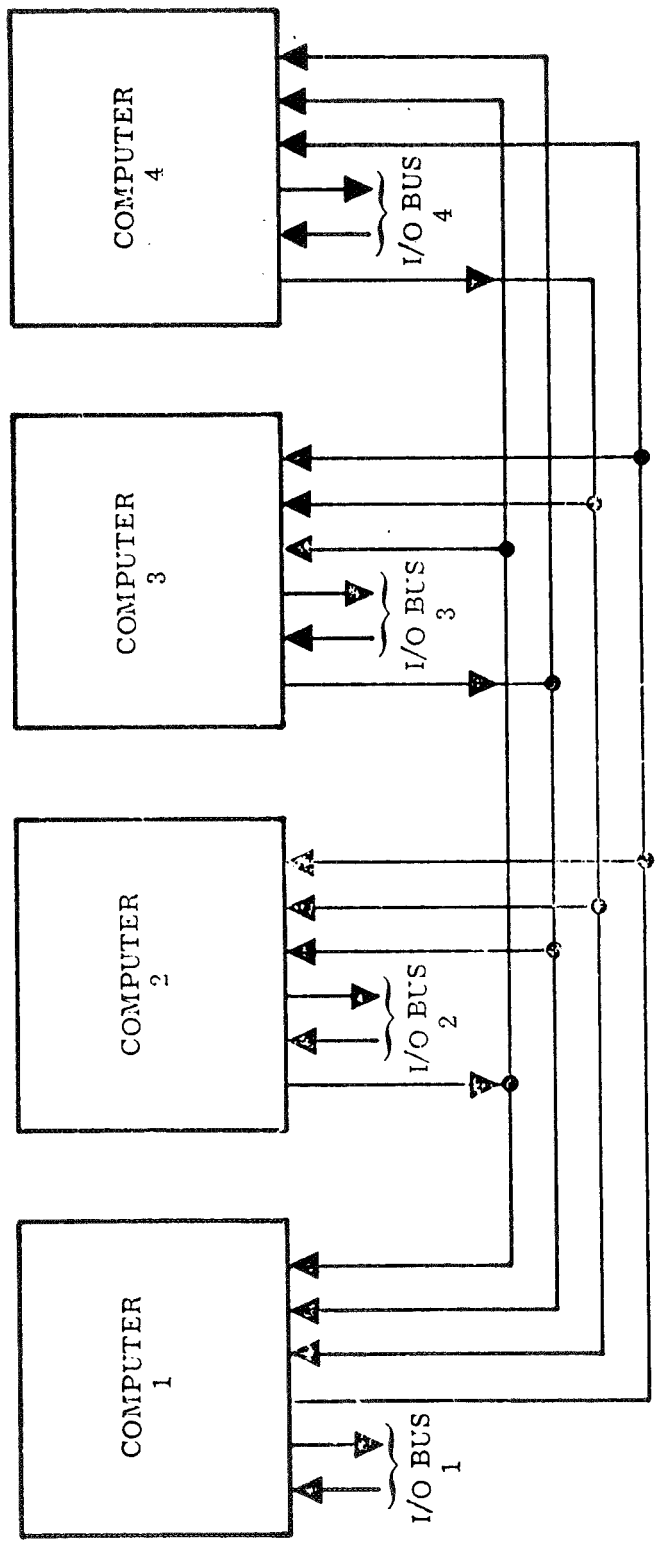

FIGURE 4-1. COMPUTER SYSTEM INTERCONNECTION DIAGRAM

4.3 (continued)

The diagram indicating the basic architecture of the VCS device and the interface between the VCS and IOP is shown in Figure 4-2. The VCS device communicates on the I/O bus to the external subsystems; it has as inputs, the outputs of the four I/O processor sections of the four computers. As shown, these inputs to the VCS may be used by the voting, comparison, or selector logic. The block containing this logic is directed by the control unit of the VCS. The control unit operates on the principle of adaptive majority logic. Its function is to control the mode of the voter-comparator-selector logic block and to decide which computers are failed or non-failed. The control unit implements its functions by means of a P matrix and a R matrix.

The P matrix (4 x 4) contains one computer's failure status opinion of another computer and the majority decision of the failure status of each computer. Essentially this matrix contains the failure status of the computer system. The failure status decision on an individual computer is derived from the other computers' failure opinion and the go/no-go self test results from the built-in test equipment in each computer. The decisions are arrived at on the basis of adaptive majority logic.

The R matrix of the control unit represents the desired mode of operation. It operates under a majority decision rule as to the selection of the mode. Further, it is adaptive in that the P matrix is used to determine which computers are failed and should be ignored in the R matrix. The R matrix is also a 4 x 4 matrix and is set directly by the computers. The R matrix logic directs the connections to the voter-comparator-selector logic to implement the mode of operation.

Since the four computers are not operated in bit sync when in the voting or comparison modes, a set of buffer shift registers are provided in the VCS to provide bit synchronous data to the voter-comparator-selector logic. The registers allow for a ± 1/2 word time out of sync operation. The I/O bus to the external subsystems is a continuous loop, providing the ability to monitor outputs of the computer on to the bus by echo check techniques of monitoring the inputs from the bus. Routing logic in the VCS device determines the destination of all input data received over the I/O bus by the VCS. This routing logic also determines which I/O processors are to receive copies of the input data from the external subsystems (e.g., in a three-way voting mode input data will be distributed to three I/O processors).

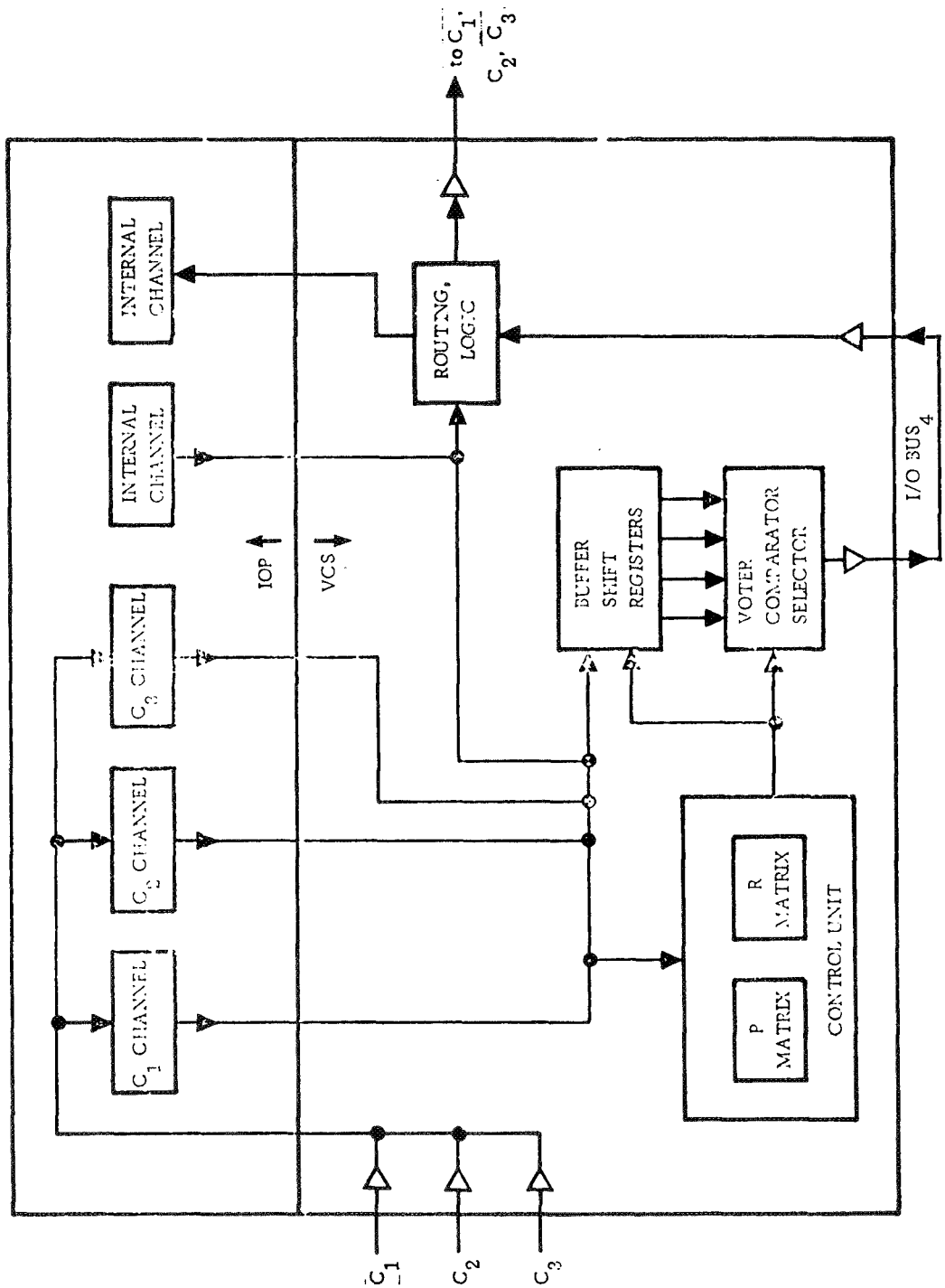

FIGURE 4-2. VCS MECHANIZATION

4.4 IOP ARCHITECTURE

The Input/Output processor (IOP) functions as an independent processor operating under a stored program in memory and capable of interfacing with the internal memory directly via the memory bus. A block diagram of the basic functions of the IOP is given in Figure 4-3. The input/output functions may be classified into three different types:

A. Type 1 - for computer-to-computer communication
B. Type 2 - for computer-to-external subsystem communication
C. Type 3 - for computer-to-parallel channel communication

Type 1 channel communications are bit serial-word serial. The channels are completely independent so that the IOP may be simultaneously receiving information from three other IOPs and sending information to these IOPs on its Type 1 output channel. The information on the Type 1 channels may contain data or commands. Further, the information may be destined for the IOP or the VCS. Likewise, the information sent out on the Type 1 channel may originate from the IOP or the VCS.

Type 2 channel communications are also bit serial-word serial. The Type 2 channel interfaces with the I/O bus that connects to the various external subsystems. The use of the Type 2 channel is completely under control of the IOP; external subsystems may only communicate with the IOP and only after being commanded to do so by the IOP. The Type 2 channel is closely interrelated to the VCS function.

In addition to these serial channels, the IOP contains a parallel I/O channel (16-bit) shown as the Type 3 channel. This channel is used for communication to devices requiring rapid data transfer (250,000 words/sec) with the computer system such as the mass storage system and the data management system. The channel operates under external control only, i.e., the IOP does not initiate data transfers over this channel. The Type 3 channel is not included in the FOOS requirement.

The IOP is set into operation by the decoding of a command and/or a control word. The commands are stored in the computer memory and are accessed according to a command program counter in the IOP. Control words are also stored in the memory and are also received from other computers in the system over the inter-computer (Type 1) bus. Control words are executed only when specified by a command or when a control word is received over the inter-computer bus. The internal and external control words mechanize the complete set of IOP information transfer operations. These include not only data transfer between computers and between computers and external subsystems, but also between computers and the VCS devices.

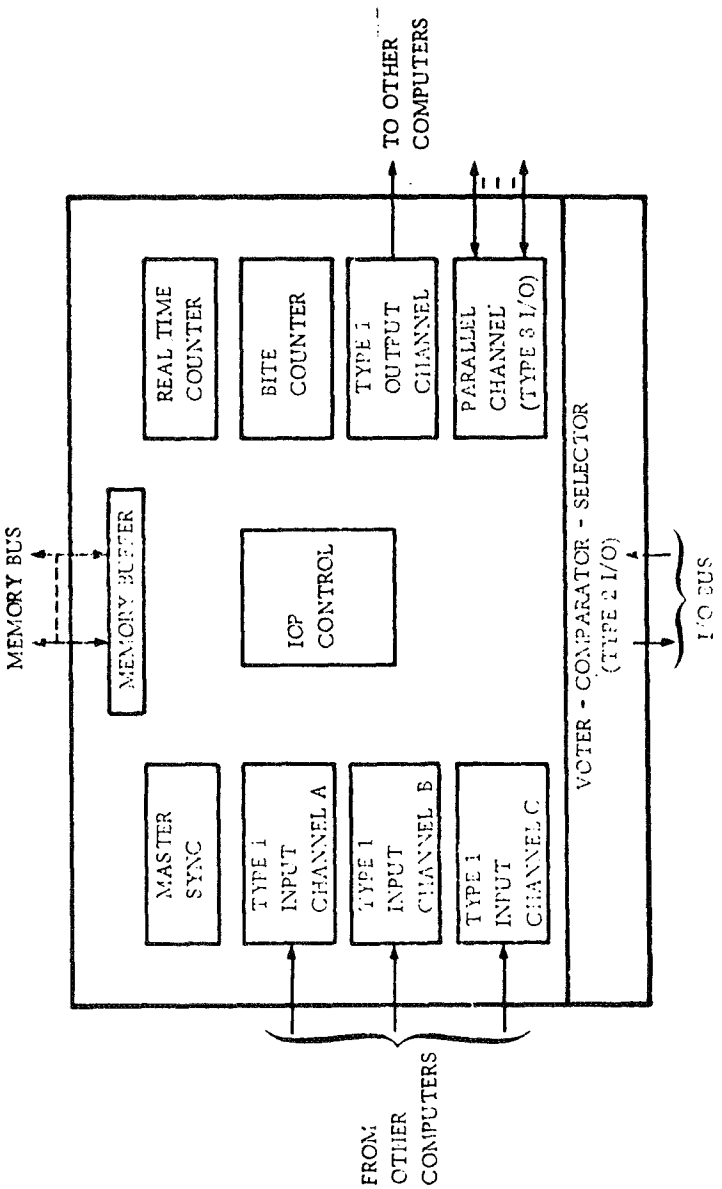

FIGURE 4-3. IOP MECHANIZATION

4.4 (continued)

The VCS device constitutes the primary means of failure detection in the computer system since an erroneous input to the voter may be readily detected. In addition, each computer contains self test capability that provides autonomous failure detection to a specified confidence level; this capability is used to aid the computer system failure reconfiguration operations. The self-test is a combination of hardware/software techniques. The IOP contains some of this hardware in the form of the BITE Counter. This counter operates such that if it is not reset periodically, it will reach a zero count and issue a computer failure signal. The counter will be reset by accessing a dedicated location in memory and loading the binary value found therein into the counter and zeroing this location after access. It is the CPU's responsibility to reload this location to keep the counter reset.

4.5 IOP/SYSTEM OPERATION

The computer system may be operated in a variety of redundancy modes. The modes are implemented by the hardware design features in the VCS. This hardware is set up and controlled by software executive control in the computer system. This executive is distributed among the four computers with the VCS hardware acting upon the software control by an adaptive majority rule. Hard core software failures are eliminated by this design approach. The VCS is designed such that the condition of its operating state and the results of voting/comparison processes may be interrogated by the executive program.

In a redundant operating mode, the data presented to the VCS must be in sync to within a word time. To compensate for factors such as drift in the clocks, machine errors (e.g., parity), and other events, the IOPs perform a re-synchronizing operation after a specified number of I/O cycles. This re-synchronizing is accomplished primarily by hardware contained in the IOP. When re-synchronization is about to take place, the IOPs send a Master Sync Control Word to each other over the Type 1 I/O channels. Special hardware times the receipt of the control words, detects any computer clock failures by determining if one has drifted out of tolerance with respect to the majority, and determines the time of synchronization. The method of synchronization eliminates a hard core clocking system.

A description of the I/O process for outputting data to the external subsystems when operating in a three-way voting mode is shown in Figure 4-4. Computers 1, 2, and 3 are shown as operating in a voting mode, computer 4 could be performing another task or in a failed state. The VCS receives three copies of the message and transmits the majority on the bus. Simultaneously, the IOPs of computers 1, 2, and 3 monitor the transmitted message by the "loop around" design of the bus. This

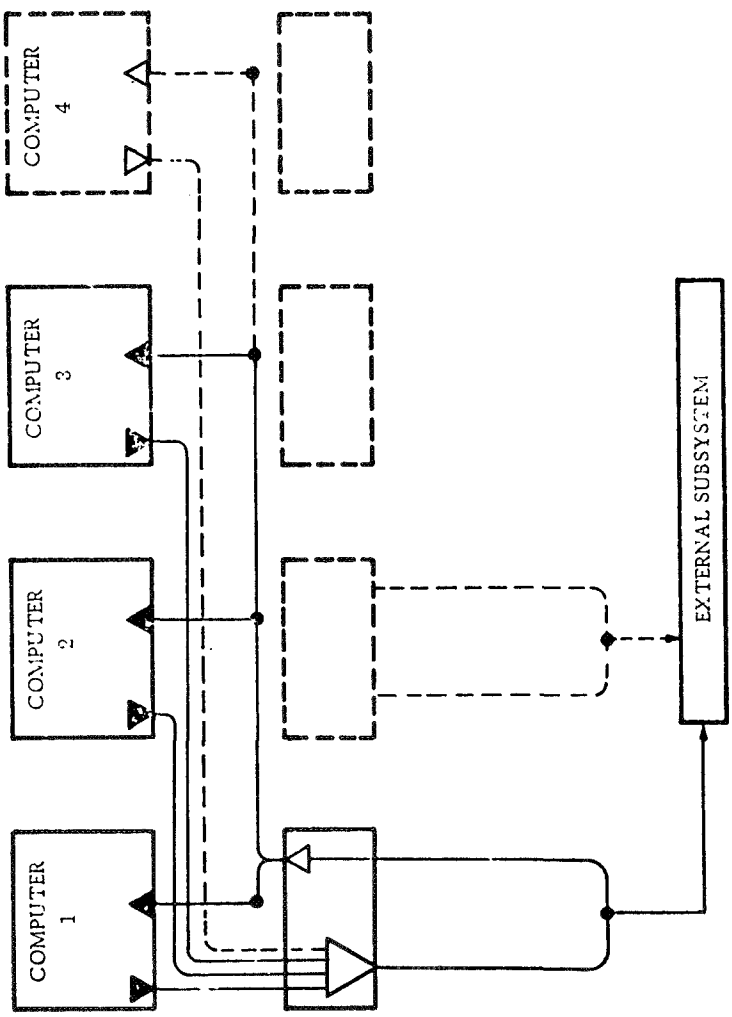

FIGURE 4-4. DATA OUTPUT PROCESS

4.5 (continued) - monitoring process consists of comparing the information sent to the VCS with that transmitted on the bus, any discrepancies are noted, and a "go" - "no-go" code is sent to the VCS by each IOP at the end of the monitoring process. Once again the majority "go/nc-go" opinion would be transmitted on the bus. The IOPs also monitor the go/no-go code transmitted on the bus to determine if they are in agreement with the majority. The IOPs contain automatic message re-transmission capabilities in case of a majority no-go opinion. Based on the monitored go/no-go code, the IOPs either proceed to the next message or re-transmit the last message. This re-transmission is attempted twice with the same VCS, if three successive transmissions fail, the IOPs then switch over to a new VCS. Three successive transmission failures with the new VCS will result in the IOPs proceeding on to the next message in the IOP sequence. The IOP also stores status words at the end of each message which indicate the occurrence of any errors or retries in the transmission process.

The process of inputting data from external subsystems for the same mode of operation, namely, three-way voting is quite similar. The command to input data to the computer systems is sent to the external subsystem over one bus. However, the data is sent to the computer system over multiple busses. Further, the data received over a bus is sent to all the IOPs; therefore, each IOP will receive three copies of the data sent to the computer system. This redundant set of input data received by each IOP is used in a software voting process by the CPU.

5.0 SELECTED COMPUTER DESIGN

5.1 CANDIDATE COMPUTERS EVALUATED

The computer system concept to meet the FOOS requirements was explained above. This concept was selected from a number of alternatives analyzed during the study. A detailed definition of various candidate computers was derived during the study to perform a quantitative evaluation. Sixteen total candidates were used in the evaluation as follows: four internal computer organizations, two technologies for mechanization, and two system concepts.

The internal organizations evaluated were a non-modular multicomputer, modular multicomputer, non-modular multiprocessor, and a modular multiprocessor. A block diagram of the latter organization is shown in Figure 5-1. It is seen that the organization is physically divided among two compartments of the spacecraft, this ground rule applied to each organization. The modules shown in solid lines are those required to satisfy the computational and failure tolerance requirements, while those in dotted lines provide expansion or spares. The two technologies used were a conventional low risk approach and an advanced higher risk approach. The former consisted of four-phase P channel MOS for logic, plated wire for memory, and conventional packaging throughout. The latter consisted of the same logic, MNOS and MOS read write semiconductor memory, and beam leaded uncased devices on ceramic substrates with the substrates assembled into large packages (approximately 1-1/2" x 2") and these packages mounted on conventional boards. Two system concepts are depicted in Figure 5-1. The first does not use the VCS device while the second does. This system concept was explained in the prior section.

The following factors were considered in the evaluation of the candidates: power, weight, volume, cost, programming ease, reconfiguration flexibility, growth potential, probability of success, transient immunity, modularity, number of interconnections, clarity of approach, subsystem/management clarity, and technology criticality. A quantitative evaluation model was derived and used on the sixteen candidates. The candidate with the highest merit was the modular multiprocessor organization, with system concept 2 (VCS device in system), and mechanized with conventional technology. The selected candidate was entitled the restructurable multicomputer since in use it is primarily used as a multicomputer, the multiprocessor paths primarily provide reconfiguration paths and growth potential.

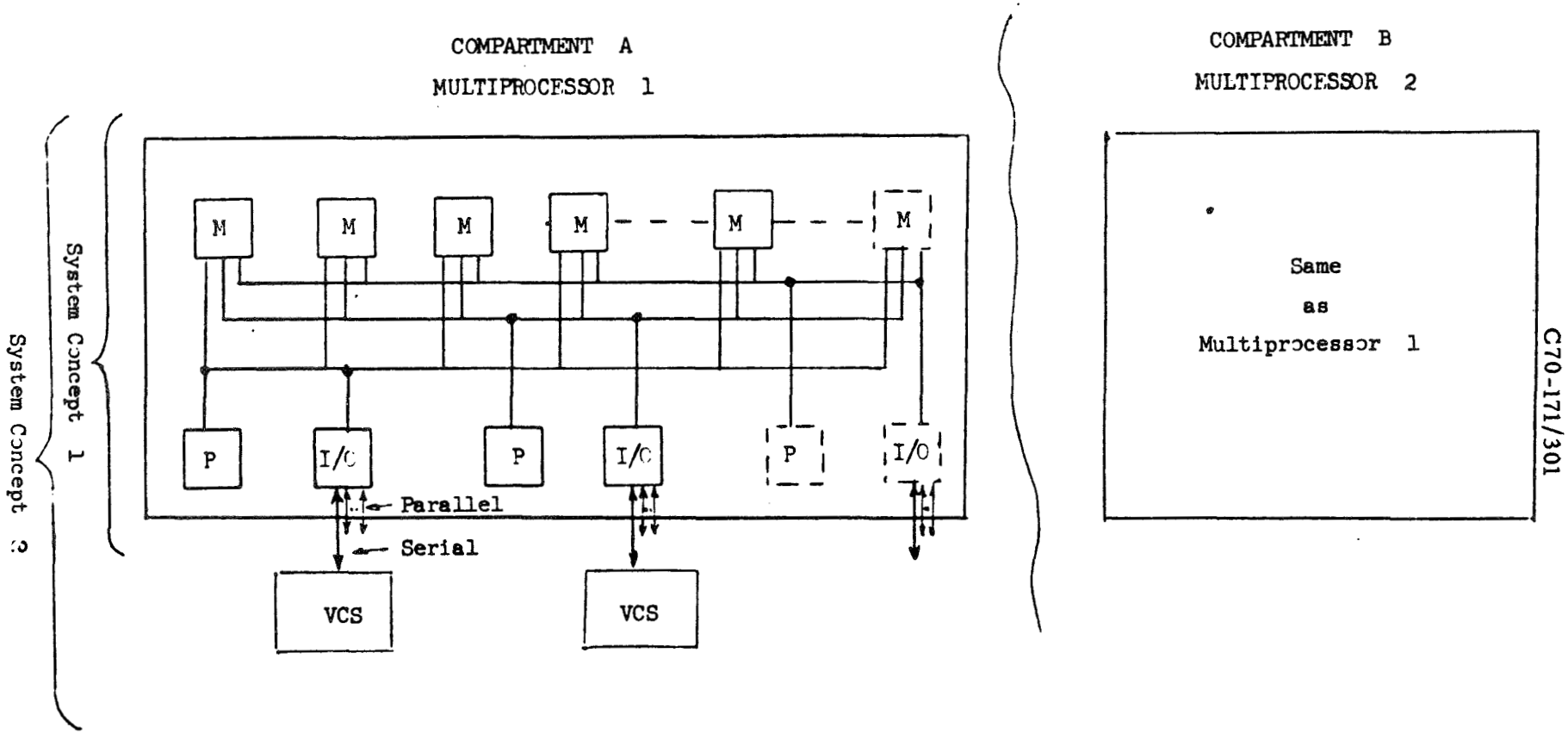

FIGURE 5-1. MODULAR MULTIPROCESSOR ORGANIZATION

5.2 SELECTED COMPUTER CHARACTERISTICS

A complete block diagram of the selected computer system with the modules required to meet the space station requirements is shown in Figure 5-2. A detailed mechanization was performed on the selected computer system. Figure 5-3 contains the internal bus structure of one of the computers in Figure 5-2. The following characteristics describe each module:

Processor Module

- Arithmetic word length: 32 bits
- Data options: 1. Fixed point
  - a. Half word
  - b. Full word
  - 2. Floating point
- Add time (incl. operand fetch from memory): 2 usec.
- Instruction Format: 16-bit and 32-bit
- Registers: General register file
- Microprogram control

Memory Module

- Capacity: 16,384 words
- Word length: 32 bits + 2 parity bits
- Multiprocessor interface with lockout control

I/O Module

- Independent processor with limited I/O handling instruction repertoire
- Baseband time division multiplexed interface to bi-directional bus
- Types 1, 2, and 3 channels as described in prior section
- VCS function as described in prior section

Memory Bus

- Common bus shared by processor and IOP

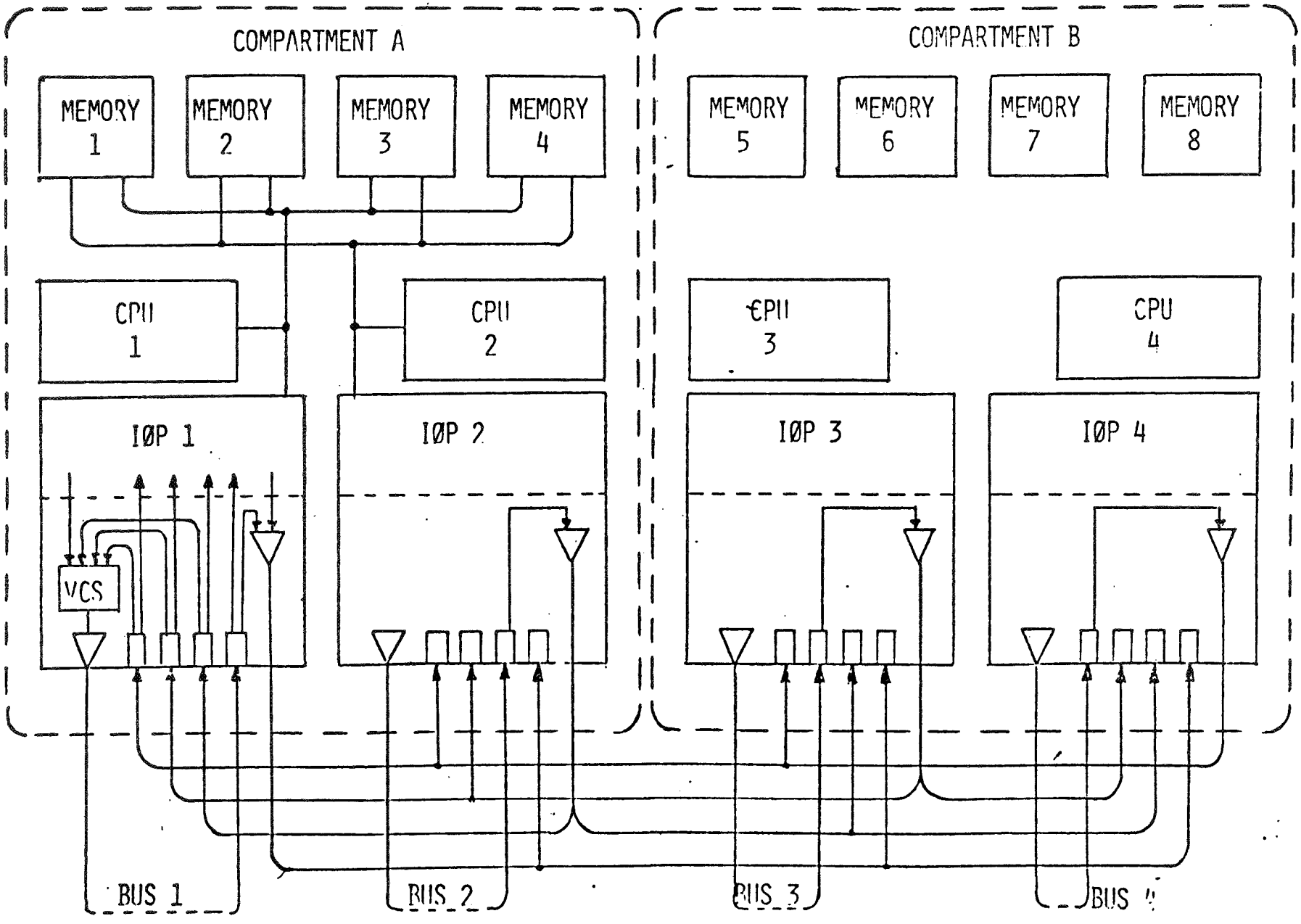

FIGURE 5-2. COMPUTER SYSTEM BLOCK DIAGRAM

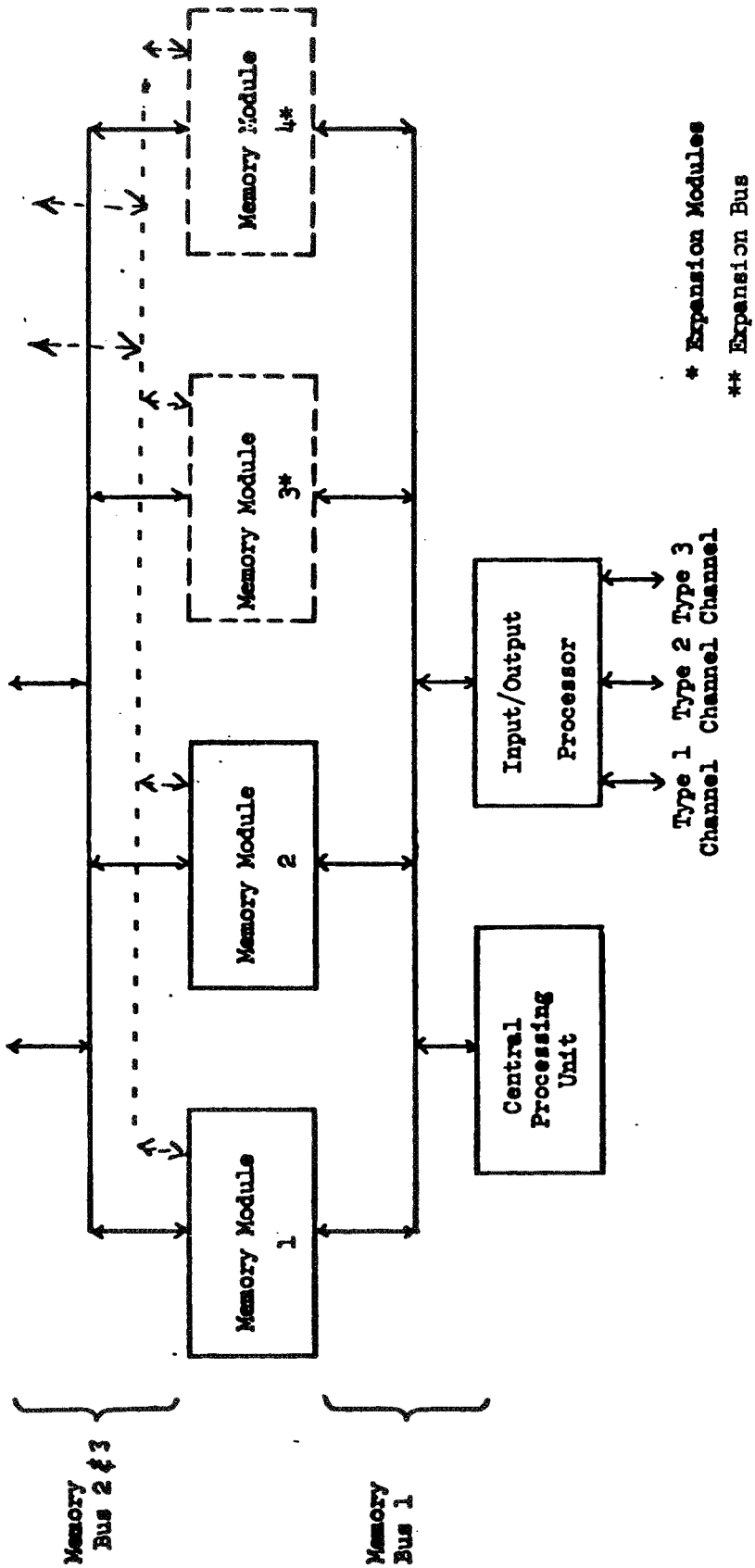

FIGURE 5-3. COMPUTER BLOCK DIAGRAM

6.0 I/O DATA BUS

6.1 SUMMARY OF STUDY ACTIVITIES

The I/O Data Bus Study was divided into six major areas of investigation and analysis. These areas or subtasks are listed below.

1. Data Transmission Requirements Analysis
2. Multiplexing Techniques
3. Modulation Techniques
4. Error Protection Techniques
5. Redundancy Considerations
6. Preferred Bus Mechanization

The requirements analysis laid the ground work for the remaining subtasks, documenting the basic requirements, assumptions and operational needs of the bus system. A data transfer rate of 88,000 bits/sec was developed from the System Analysis and Trade-offs Tasks. This represents the volume of required useful data and does not include any overhead for transmission control nor growth requirements. 1 MHz bit rate was established as a reasonable design requirement since it is well within the state-of-the-art and permits significant capability for growth.

The subtasks (2), (4), and (5) comprised over one-half the effort and were closely interrelated. Major emphasis was directed to error protection. Error protection techniques that have been examined include the following: (1) simple parity checking, (2) complex parity checking, (3) re-transmission techniques, (4) Hamming codes, (5) Bose-Chaudhuri codes, (6) fire codes, (7) other block and conventional coding techniques, and (8) combination of the above techniques.

The overall results of the first five subtasks were compiled and summarized as part of subtask (6). The preferred mechanization and detailed baseline design for the bus elements and the standard interface unit (SIU) are documented in this Volume II of this report. A brief summary of the final results of this study is presented below.

6.2 RECOMMENDED I/O DATA BUS MECHANIZATION

The I/O data bus will operate as four separate, independent communication links. The operation of each individual data bus will be under complete computer control in a request-acknowledge format. Communication on the bus will be in messages, each message headed by two control words and ending with a check word. The number of words in a data message is variable up to a maximum of 63 total words.

6.2 (continued)

The baseline method of data transmission on each bus will be baseband, utilizing bi-phase level encoding (Manchester). The data links will be twisted pair shielded cables, balanced and terminated. Each standard interface unit (SIU) will be coupled via transformers to the data link and resistor isolated from the data line for short circuit protection. The data link will be a true party line configuration. Clocking for each SIU will be derived from the received data utilizing a higher frequency clock source provided for the Local Processor. A data synchronization code will be used for group synchronization at each SIU. A different synchronization code will be used for communications to the computer ruling out any communication between SIUs on the same party line.

Two-dimensional simple odd parity checks will be used on all messages for error protection. An error detection-request re-transmission scheme will be used to ensure correct data transfer to each SIU. The re-transmission will be under computer control and mode sensitive to allow full computer control of the bus system throughout. The possibility of simple forward single error correction plus double error detection is available with this error control format to improve throughout at any time.

Each SIU will have multiple I/O bus lines and circuitry to allow multiple independent receptions of the same data if desired. This level of hardware redundancy at the SIU also allows SIU reconfiguration after SIU or bus failures. The SIU design is such that no single SIU failure will cause loss of any data link. Redundant, independent, transmitter enable circuitry and time-outs are used for this purpose.

7.0 SOFTWARE AND SIMULATION

The software and simulation task had a three-fold objective.

1. Design and develop a software simulation of the selected computer system design developed during the course of the study. The simulation should be suitable for use as a tool for evaluation/demonstration of preliminary design concepts and techniques.

2. Design and develop the software routines necessary to operate the simulated computer system in a FOOS environment.

3. Utilize the simulation system to debug the software and system design and to demonstrate/evaluate the feasibility and functional performance of the selected computer/software system.

The Reconfigurable G&C Computer (RGC) simulation system which was developed during this task consists of two computer programs: (1) the assembly program and (2) the RGC Computer System Simulator program. These programs are written in the FORTRAN IV language and are compatible from a language standpoint with most medium and large scale general purpose computer systems; among them the IBM S360, CDC 6600, XDS Sigma 5/7, and Univac 1108. The programs have been executed on all the above systems except the 1108.

The two programs are executed independently. The assembly program is used to process programs written in a symbolic assembly language for execution on the simulated RGC computer system and convert them to a format suitable for input to the simulator program. Additionally, the assembly program produces a printed listing of the programs. The simulator program simulates functional operation of the selected RGC computer system design by "executing" the assembled RGC computer programs and providing a printed trace of CPU, IOP, and memory activity and interaction. Simulation is performed at a functional, machine-register level and does not duplicate specific logic or circuit mechanizations.

The software routines programmed for execution on the simulation system are referred to as the RGC Software System and constitute a limited "operating" system for the simulated RGC computer system. This software is composed of three sub-programs: (1) Executive program, (2) Input/Output program, and (3) Resource Controller program. Except for format differences, these routines are identical to programs which might be implemented in an actual guidance and control computer to perform the executive, input/output and reconfiguration functions.

7.0 (continued)

Operation of an integrated multicomputer system presents some unique problems in the area of overall system control, sequencing, and mode/status maintenance. (The term integrated system is used here to exclude multi-computer systems which are essentially operated as a group of independent non-interacting units).

The major problems arise from considerations of the effect of processor failures on overall system performance, and are primarily related to determining where to assign primary system control and how to reassign it in the event of a failure. The reassignment problem is particularly troublesome since reassignment implies a higher authority and the unit or function being reassigned is by definition itself the highest authority in the system. In systems where fault tolerance is not a primary concern, these problems are normally overcome by some variation of a "distributed" software executive. That is, the system level executive functions are shared by the multiple computers with some limited set of simple indicators (such as watchdog timers, parity checks, etc.) being used to trigger system degradation or reconfiguration.

In most systems designed primarily for fault-tolerance, a "hard core" control unit is usually employed in one form or another which has responsibility for primary configuration control. Internal circuit redundancy is used to increase the survivability of this hard-core unit.

The philosophy of operation employed in the RGC software system is a logical extension of the concepts developed in the overall system design and stems from the desire to achieve extremely high failure detection/reconfiguration probabilities without the necessity for unique, special purpose, hard-core hardware.

A redundant, majority-controlled software system is employed. Though it is resident in all computers, it is not "distributed" in the normal sense, since the entire function is duplicated identically and computed redundantly in all computers. Each computer therefore has equal status in terms of system control and decisions are achieved through a majority voting process. The highest level of system control - the decisions as to which computers are operational - is accomplished in the VCSes contained in each IOP. Each computer's opinion of the health of all computers is transmitted to the VCSes and the VCS logic performs an adaptive majority vote on this data. The result of this vote is in turn monitored by each computer and accepted as the current system status. Lower-level decisions are resolved through a software voting process which involves the computers exchanging opinions and accepting the resultant majority opinion.

7.0 (continued)

The underlying purpose for the development and use of the simulation system was two-fold:

1. To provide a tool which could be used for development and evaluation of computer/software system designs oriented toward fault-tolerant system operation.
2. Use the tool to develop and evaluate the system design proposed to satisfy the FOOS requirements.

Use of the simulation system during the course of this study involved four primary activities.

1. Refining and solidifying the functional design characteristics of the selected system being evaluated during the study.
2. Debugging and evaluating operation of the simulation system.
3. Debugging and refining the software for the selected system design.
4. Evaluating overall system performance using fault simulation.

The simulation activities, particularly number 4, are somewhat open-ended in that system evaluation and design refinement efforts can be extended almost indefinitely particularly in the area of fault simulation. The primary goal during this study was to provide a reasonable level of confidence in the feasibility and functional performance of the proposed system in terms of satisfying the FOOS requirements. Although the system level fault injection and recovery was limited to a few simulation runs, it is felt that the primary goals were accomplished and the desired confidence in the system fault tolerance was attained.

8.0 POWER DISTRIBUTION

One of the study tasks was to investigate and recommend a preferred power distribution method for the G&C system. The requirement was that the distribution system operation be not degraded by a power failure at the modular level.

Redundant power sources of MIL-STD-704A quality were assumed to be available on four redundant power busses. An investigation of MIL-STD-704A power revealed that it imposes severe design constraints on power converter design. A recommended solution is to provide "computer grade" DC power which is to be held within more reasonable limits, e.g., 24V to 32V.

Source and load isolation after failures were of principal concern during the study. Several load and source isolation methods were investigated and their failure mode effects in a generalized redundant power distribution system were examined. This analysis lead to two conclusions: (1) the only isolator that works for all failure modes is a series switch which fails in an open condition, (2) if sources and loads have certain limited failure modes, then other isolator types may permit the FOOS criterion be met with something less than brute force quadruple redundancy.

The general investigation of various isolation types was followed by an examination of isolation devices and their failure modes. Diodes for DC applications include computer diodes, diffused diodes, ion implantation diodes and Schottky barrier hot carrier diodes. For AC systems, magnetic isolators of three types were investigated. These were a simple magnetic amplifier, a four aperture magnetic switch developed by Stanford Research Institute for Jet Propulsion Laboratory under NASA contract, and the parametric magnetic device called Paraformer TM, a product of Wanlass Electric Co. Also, solid state controllers under development for aircraft applications were examined, and finally, electromechanical relays were considered briefly for comparison purposes.

The solid state controllers are recommended for the Space Station power distribution system. They are substantially superior to other types from the standpoint of volume and weight. They have as good efficiency as the magnetic devices but are poorer than the nearly lossless conventional circuit breaker. Their present progress of development for aircraft systems has been quite rapid, therefore, their use in the Space Station does not appear to introduce any new development risks. Because of the higher power loss in switching transistors, the solid state devices require careful attention to cooling methods.

The recommended system is essentially a distributed system with load controllers packaged with the subsystem load at the interface point with the Electrical Power Subsystem. The power control logic is to be located as a separate module at the Local Processor. The Local Processor will have its own load controller which receives control signals via I/O data bus.